CLAIMS:

Sub A2

1. A computer network comprising:

a first edge device coupled to a first private network, the first edge device configured to create a first table with information of member networks reachable through the first edge device, the first table being stored in a first database;

a second edge device coupled to a second private network, the second edge device configured to create a second table with information of member networks reachable through the second edge device, the second table being stored in a second database;

wherein, the first and second edge devices enable secure communication between the first and second private networks, and the first edge device shares the first table with the second edge device and the second edge device shares the second table with the first edge device.

2. The computer network of claim 1, wherein the first edge device includes logic for:

receiving a new route information;

storing the new route information in the first database; and

transmitting a portion of the new route information to the second edge device.

3. The computer network of claim 2, wherein the portion of the new route information is a route name.

4. The computer network of claim 2, wherein the second edge device includes logic for:

receiving the portion of the new route information;

accessing the first database based on the portion of the new route information;

retrieving the new route information from the first database; and

storing the retrieved route information in the second database.

5. The computer network of claim 1, wherein communication between the first and second networks is managed according to a security policy associated with the networks.

6. The computer network of claim 5, wherein the security policy is defined for a security group providing a hierarchical organization of the group, the group including member networks, users allowed to access the member networks, and a rule controlling access to the member networks.

7. The computer network of claim 6, wherein each member network has full connectivity with all other member networks and the security policy defined for the security policy group is automatically configured for each connection.

8. The computer network of claim 6, wherein the security policy provides encryption of traffic among the member networks and the rule is a firewall rule providing access control of the encrypted traffic among the member networks.

9. In a computer network including a first edge device coupled to a first private network and a second edge device coupled to a second private network, the first and second edge devices enabling secure communication between the first and second private networks, a method for gathering membership information comprising:

creating a first table with information of member networks reachable through the first edge device,

storing the first table in a first database;

creating a second table with information of member networks reachable through the second edge device;

storing the second table in a second database;

sharing the first table with the second edge device; and

sharing the second table with the first edge device.

10. The method of claim 9 further comprising:

receiving a new route information;

storing the new route information in the first database; and

transmitting a portion of the new route information to the second edge device.

11. The method of claim 10, wherein the portion of the new route information is a route name.

12. The method of claim 10 further comprising:

receiving the portion of the new route information;

accessing the first database based on the portion of the new route information;

retrieving the new route information from the first database; and

storing the retrieved route information in the second database.

13. The method of claim 9, wherein communication between the first and second networks is managed according to a security policy associated with the networks.

14. The method of claim 13 further comprising defining the security policy for a security policy group, the group providing a hierarchical organization of the group including member networks, users allowed to access the member networks, and a rule controlling access to the member networks.

15. The method of claim 14, wherein each member network has full connectivity with all other member networks and the security policy defined for the security policy group is automatically configured for each connection.

16. The method of claim 14, wherein the security policy provides encryption of traffic among the member networks and the rule is a firewall rule providing access control of the encrypted traffic among the member networks.